

1 **CLAIMS**

2 1. In a computer system, a method for providing application security
3 threat-modeling, the method comprising:

4 defining a plurality of model components to represent respective
5 elements of an application, each model component comprising a respective set
6 of potential security threats;

7 interconnecting the model components to form a logical model of the
8 application; and

9 analyzing one or more of the potential security threats in terms of the
10 model components in the logical model.

11
12 2. A method as recited in claim 1, wherein the model components
13 comprise a module, a port, a store, or a wire.

14
15 3. A method as recited in claim 1, wherein the potential security
16 threats comprise at least one subset of authentication, authorization, auditing,
17 privacy, integrity, availability, and non-repudiation.

18
19 4. A method as recited in claim 1, wherein defining the model
20 components further comprises

21 determining the respective security threat characteristics for a
22 component of the model components based on the components corresponding
23 functionality in the application.
24
25

1 5. A method as recited in claim 1, wherein analyzing one or more of
2 the potential threats in terms of the model components further comprises:
3 selecting a particular component of the model components; and
4 responsive to selecting the particular component, displaying each other
5 component of the model components that comprise at least a subset of similar
6 potential security threats as the particular component.

7
8 6. A method as recited in claim 1, wherein analyzing one or more of
9 the potential threats in terms of the model components further comprises:
10 selecting a particular component of the model components; and
11 responsive to selecting the particular component, displaying each other
12 component of the model components that comprise at least a subset of similar
13 addressed security threats as the particular component.

14
15 7. A method as recited in claim 1, wherein analyzing one or more of
16 the potential security threats in terms of the model components in the logical
17 model further comprises:
18 selecting a particular threat of the potential threats to indicate that the
19 particular threat requires a threat mitigating implementation in a particular
20 mode component of the model components, the particular threat corresponding
21 to the particular model component.

22
23 8. A method as recited in claim 5, wherein selecting the particular
24 threat further comprises identifying a priority that corresponds to the threat
25 mitigating implementation.

1 **9.** A method as recited in claim 7, wherein selecting the particular
2 threat further comprises identifying a desired level of strength technology with
3 which to mitigate the particular threat.

4
5 **10.** A method as recited in claim 1, wherein selecting the particular
6 threat further comprises selecting a particular technology with which to
7 mitigate the one or more potential threats in a physical implementation of the
8 application.

9
10 **11.** A computer-readable medium comprising computer-executable
11 instructions for providing application security threat-modeling, the computer-
12 executable instructions comprising instructions for:

13 defining a plurality of model components to represent respective
14 elements of an application, each model component comprising a respective set
15 of potential security threats;

16 interconnecting the model components to form a logical model of the
17 application; and

18 analyzing one or more of the potential security threats in terms of the
19 model components in the logical model.

20
21 **12.** A computer-readable medium as recited in claim 11, wherein the
22 model components comprise a module, a port, a store, or a wire.

23
24 **13.** A computer-readable medium as recited in claim 11, wherein the
25 potential security threats comprise at least one subset of authentication,
authorization, auditing, privacy, integrity, availability, and non-repudiation.

1 **14.** A computer-readable medium as recited in claim 11, wherein the
2 computer-executable instructions for defining the model components further
3 comprise instructions for determining the respective security threat
4 characteristics for a component of the model components based on the
5 components corresponding functionality in the application.

6
7 **15.** A computer-readable medium as recited in claim 11, wherein the
8 computer-executable instructions for analyzing one or more of the potential
9 threats in terms of the model components further comprise instructions for:

10 selecting a particular component of the model components; and
11 responsive to selecting the particular component, displaying each other
12 component of the model components that comprise at least a subset of similar
13 potential security threats as the particular component.

14
15 **16.** A computer-readable medium as recited in claim 11, wherein the
16 computer-executable instructions for analyzing one or more of the potential
17 threats in terms of the model components further comprise instructions for:

18 selecting a particular component of the model components; and
19 responsive to selecting the particular component, displaying each other
20 component of the model components that comprise at least a subset of similar
21 addressed security threats as the particular component.

1 **17.** A computer-readable medium as recited in claim 11, wherein the
2 instructions for analyzing one or more of the potential security threats in terms
3 of the model components in the logical model further comprise instructions for:

4 selecting a particular threat of the potential threats to indicate that the
5 particular threat requires a threat mitigating implementation in a particular
6 mode component of the model components, the particular threat corresponding
7 to the particular model component.

8
9 **18.** A computer-readable medium as recited in claim 17, wherein the
10 computer-executable instructions for selecting the particular threat further
11 comprise instructions for identifying a priority that corresponds to the threat
12 mitigating implementation.

13
14 **19.** A computer-readable medium as recited in claim 17, wherein the
15 computer-executable instructions for selecting the particular threat further
16 comprise instructions for identifying a desired level of strength technology with
17 which to mitigate the particular threat.

18
19 **20.** A computer-readable medium as recited in claim 11, wherein the
20 computer-executable instructions for selecting the particular threat further
21 comprise instructions for selecting a particular technology with which to
22 mitigate the one or more potential threats in a physical implementation of the
23 application.

1 **21.** A device comprising:

2 a memory comprising computer-executable instructions for providing
3 application security threat-modeling;

4 a processor that is operatively coupled to the memory, the processor
5 being configured to fetch and execute the computer-executable instructions
6 from the memory, the computer-executable instructions comprising instructions
7 for:

8 defining a plurality of model components to represent respective
9 elements of an application, each model component comprising a respective set
10 of potential security threats;

11 interconnecting the model components to form a logical model of
12 the application; and

13 analyzing one or more of the potential security threats in terms of
14 the model components in the logical model.

15
16 **22.** A device as recited in claim 21, wherein the model components
17 comprise a module, a port, a store, or a wire.

18
19 **23.** A device as recited in claim 21, wherein the potential security
20 threats comprise at least one subset of authentication, authorization, auditing,
21 privacy, integrity, availability, and non-repudiation
22
23
24
25

1 **24.** A device as recited in claim 21, wherein the computer-executable
2 instructions for defining the model components further comprise instructions
3 for determining the respective security threat characteristics for a component of
4 the model components based on the components corresponding functionality in
5 the application.

6
7 **25.** A device as recited in claim 21, wherein the computer-executable
8 instructions for analyzing one or more of the potential threats in terms of the
9 model components further comprise instructions for:

10 selecting a particular component of the model components; and
11 responsive to selecting the particular component, displaying each other
12 component of the model components that comprise at least a subset of similar
13 potential security threats as the particular component.

14
15 **26.** A device as recited in claim 21, wherein the computer-executable
16 instructions for analyzing one or more of the potential threats in terms of the
17 model components further comprise instructions for:

18 selecting a particular component of the model components; and
19 responsive to selecting the particular component, displaying each other
20 component of the model components that comprise at least a subset of similar
21 addressed security threats as the particular component.

1 **27.** A device as recited in claim 21, wherein the instructions for
2 analyzing one or more of the potential security threats in terms of the model
3 components in the logical model further comprise instructions for:

4 selecting a particular threat of the potential threats to indicate that the
5 particular threat requires a threat mitigating implementation in a particular
6 mode component of the model components, the particular threat corresponding
7 to the particular model component.

8
9 **28.** A device as recited in claim 27, wherein the computer-executable
10 instructions for selecting the particular threat further comprise instructions for
11 identifying a priority that corresponds to the threat mitigating implementation.

12
13 **29.** A device as recited in claim 27, wherein the computer-executable
14 instructions for selecting the particular threat further comprise instructions for
15 identifying a desired level of strength technology with which to mitigate the
16 particular threat.

17
18 **30.** A device as recited in claim 27, wherein the computer-executable
19 instructions for selecting the particular threat further comprise instructions for
20 selecting a particular technology with which to mitigate the one or more
21 potential threats in a physical implementation of the application.

1 **31.** A user interface for application security threat-modeling, the user
2 interface comprising:

3 means for displaying and interconnecting a plurality of model
4 components to design a logical model of an application, at least a subset of the
5 model components comprising a corresponding set of potential security threat
6 characteristics;

7 means for specifying a component of the model components; and

8 means for addressing one or more of the potential security threats in
9 terms of the model components in the logical model.

10
11 **32.** A user interface as recited in claim 31, wherein the model
12 components comprise a module, a port, a store, or a wire.

13
14 **33.** A user interface as recited in claim 31, wherein the
15 corresponding security threat characteristics comprise at least one subset of
16 authentication, authorization, auditing, privacy, integrity, availability, and non-
17 repudiation.

18
19 **34.** A user interface as recited in claim 31, further comprising:
20 means for selecting a priority that corresponds to the one or more
21 potential security threats.

22
23 **35.** A user interface as recited in claim 31, further comprising:
24 means for specifying a desired level of strength of technology with
25 which to mitigate the one or more potential security threats.

1 **36.** A user interface as recited in claim 31, further comprising means
2 for selecting a particular technology with which to mitigate the one or more
3 potential security threats in a physical implementation of the application.
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25